

# Отчёт по лабораторной работе №6

дисциплина: Информационная безопасность

Зорин Илья Михайлович

## Содержание

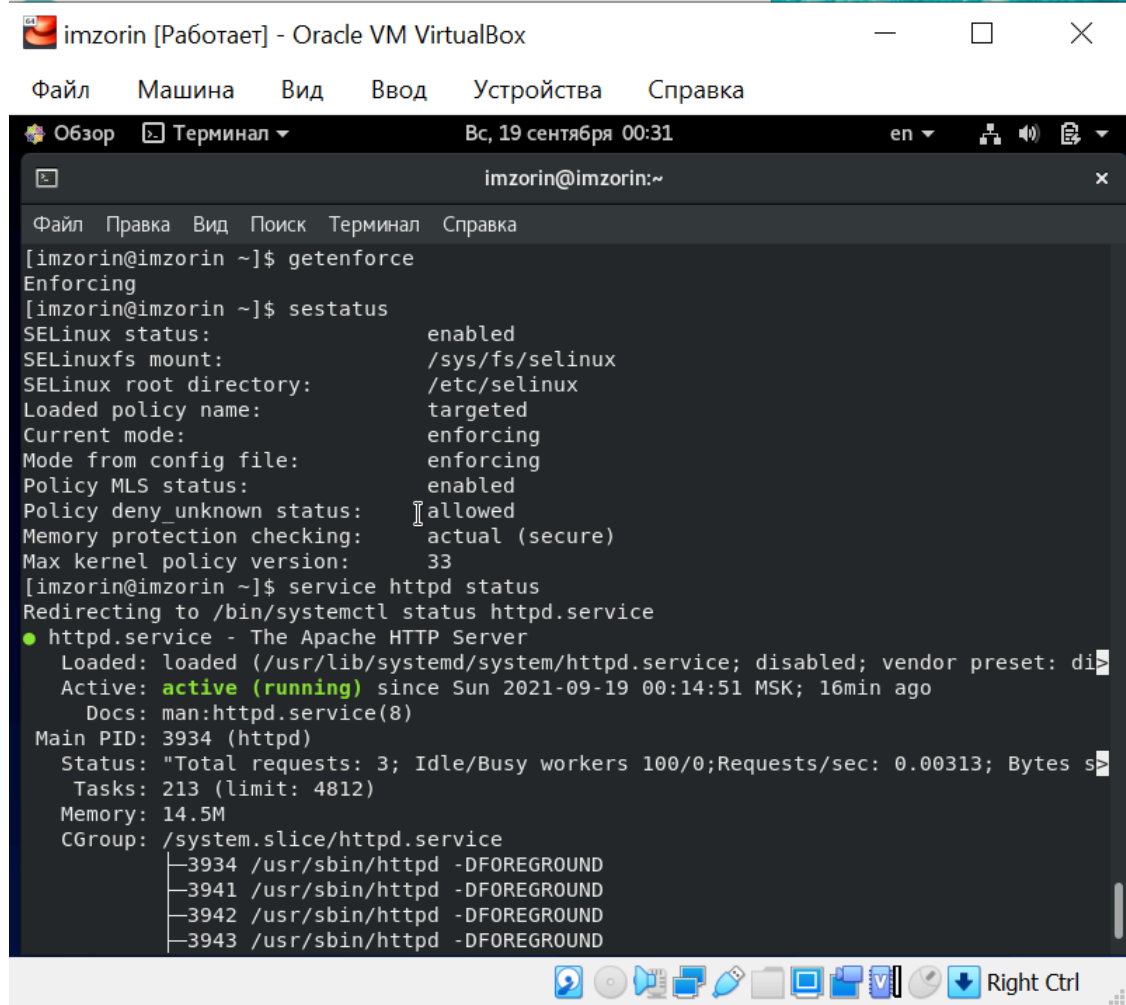
### Цель работы

Развить навыки администрирования ОС Linux. Получить первое практическое знакомство с технологией SELinux. Проверить работу SELinux на практике совместно с веб-сервером Apache.

### Выполнение лабораторной работы

1. Вошёл в систему с полученными учётными данными и убедился, что SELinux работает в режиме enforcing политики targeted. Обратился с помощью браузера к веб-серверу, запущенному на компьютере, и убедился, что

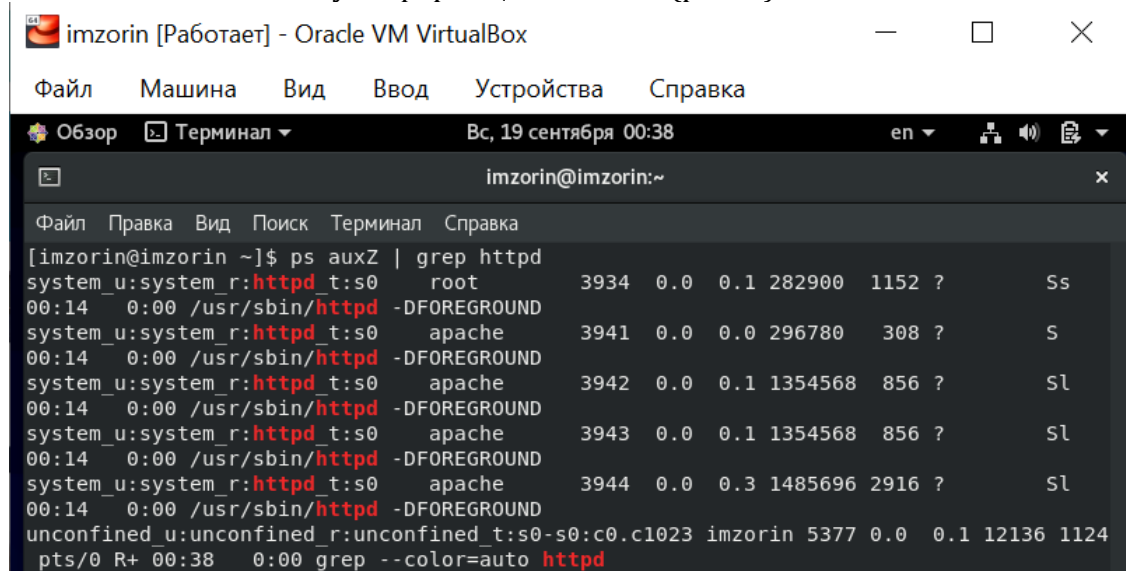
последний работает (рис. 1).



The screenshot shows a terminal window titled "imzorin [Работает] - Oracle VM VirtualBox". The terminal output is as follows:

```
[imzorin@imzorin ~]$ getenforce
Enforcing
[imzorin@imzorin ~]$ sestatus
SELinux status:                enabled
SELinuxfs mount:                /sys/fs/selinux
SELinux root directory:         /etc/selinux
Loaded policy name:              targeted
Current mode:                    enforcing
Mode from config file:          enforcing
Policy MLS status:              enabled
Policy deny_unknown status:     allowed
Memory protection checking:      actual (secure)
Max kernel policy version:      33
[imzorin@imzorin ~]$ service httpd status
Redirecting to /bin/systemctl status httpd.service
● httpd.service - The Apache HTTP Server
   Loaded: loaded (/usr/lib/systemd/system/httpd.service; disabled; vendor preset: disabled)
   Active: active (running) since Sun 2021-09-19 00:14:51 MSK; 16min ago
     Docs: man:httpd.service(8)
   Main PID: 3934 (httpd)
    Status: "Total requests: 3; Idle/Busy workers 100/0; Requests/sec: 0.00313; Bytes served/sec: 0.00000"
   Tasks: 213 (limit: 4812)
  Memory: 14.5M
    CGroup: /system.slice/httpd.service
            └─3934 /usr/sbin/httpd -DFOREGROUND
              └─3941 /usr/sbin/httpd -DFOREGROUND
                └─3942 /usr/sbin/httpd -DFOREGROUND
                  └─3943 /usr/sbin/httpd -DFOREGROUND
```

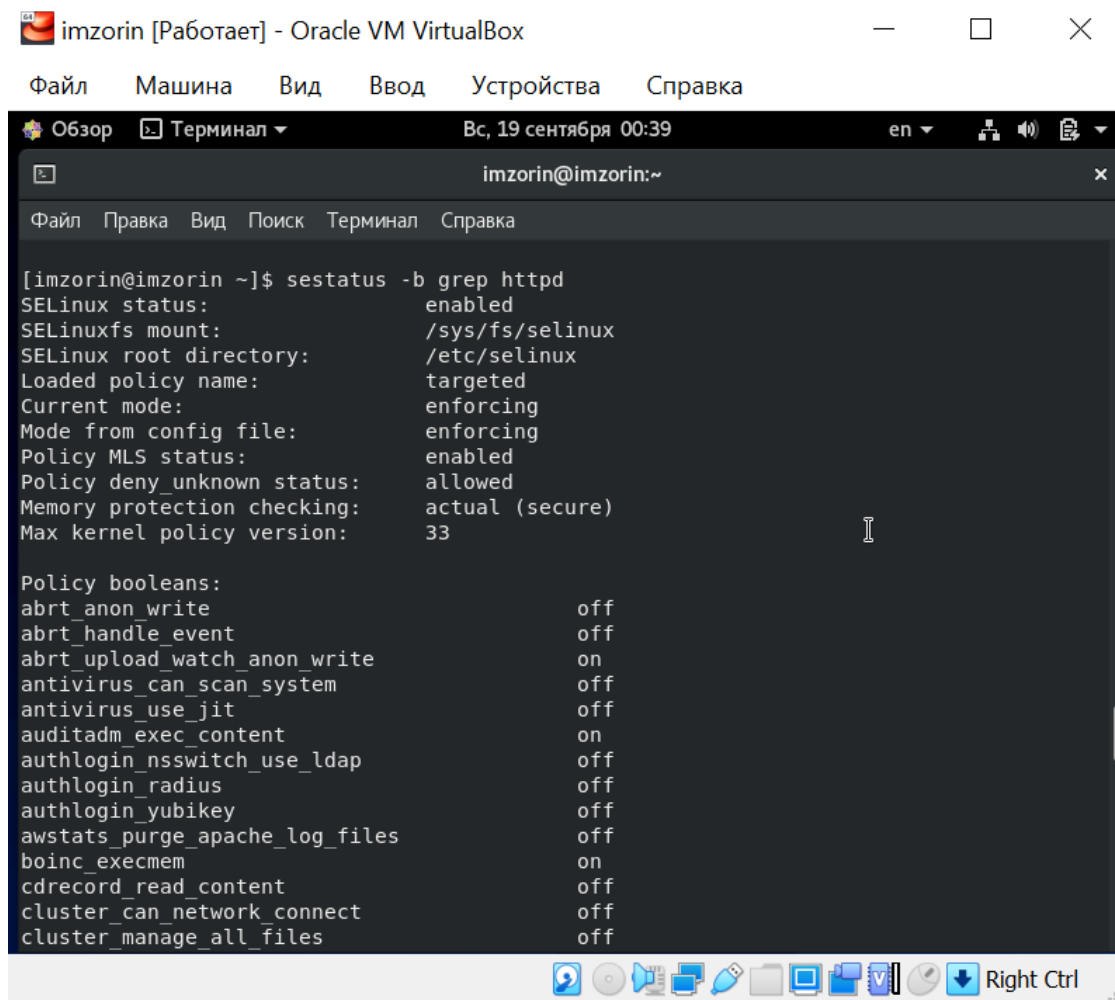
2. Нашёл веб-сервер Apache в списке процессов, определил его контекст безопасности и занёс эту информацию в отчёт (рис. 2).



The screenshot shows a terminal window titled "imzorin [Работает] - Oracle VM VirtualBox". The terminal output is as follows:

```
[imzorin@imzorin ~]$ ps auxZ | grep httpd
system_u:system_r:httpd_t:s0      root          3934  0.0  0.1 282900  1152 ?        Ss
00:14  0:00 /usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0      apache        3941  0.0  0.0 296780   308 ?        S
00:14  0:00 /usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0      apache        3942  0.0  0.1 1354568  856 ?        Sl
00:14  0:00 /usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0      apache        3943  0.0  0.1 1354568  856 ?        Sl
00:14  0:00 /usr/sbin/httpd -DFOREGROUND
system_u:system_r:httpd_t:s0      apache        3944  0.0  0.3 1485696 2916 ?        Sl
00:14  0:00 /usr/sbin/httpd -DFOREGROUND
unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023 imzorin 5377 0.0  0.1 12136 1124
pts/0 R+ 00:38  0:00 grep --color=auto httpd
```

3. Посмотрел текущее состояние переключателей SELinux для Apache (рис. 3).



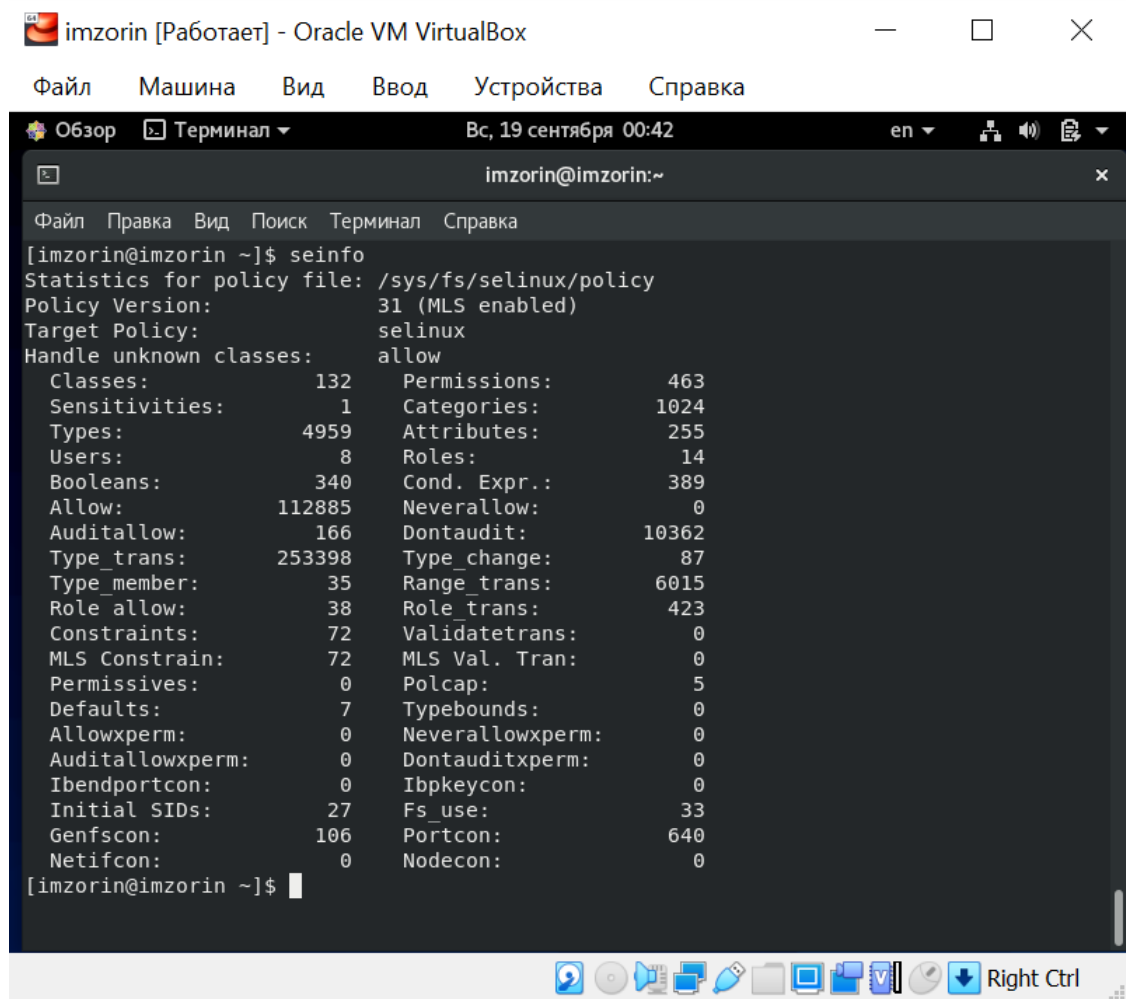
The screenshot shows a terminal window titled "imzorin [Работает] - Oracle VM VirtualBox". The terminal displays the output of the command `sestatus -b grep httpd`. The output is as follows:

```
[imzorin@imzorin ~]$ sestatus -b grep httpd
SELinux status:                enabled
SELinuxfs mount:              /sys/fs/selinux
SELinux root directory:      /etc/selinux
Loaded policy name:          targeted
Current mode:                 enforcing
Mode from config file:       enforcing
Policy MLS status:           enabled
Policy deny_unknown status:   allowed
Memory protection checking:   actual (secure)
Max kernel policy version:    33

Policy booleans:
abrt_anon write                off
abrt_handle_event              off
abrt_upload_watch_anon_write   on
antivirus_can_scan_system      off
antivirus_use_jit              off
auditadm_exec_content          on
authlogin_nsswitch_use_ldap     off
authlogin_radius               off
authlogin_yubikey              off
awstats_purge_apache_log_files off
boinc_execmem                  on
cdrecord_read_content           off
cluster_can_network_connect     off
cluster_manage_all_files       off
```

The terminal window has a menu bar with "Файл", "Машина", "Вид", "Ввод", "Устройства", and "Справка". The terminal itself has a menu bar with "Файл", "Правка", "Вид", "Поиск", "Терминал", and "Справка". The status bar at the bottom of the terminal shows the date and time "Вс, 19 сентября 00:39", the language "en", and a "Right Ctrl" button.

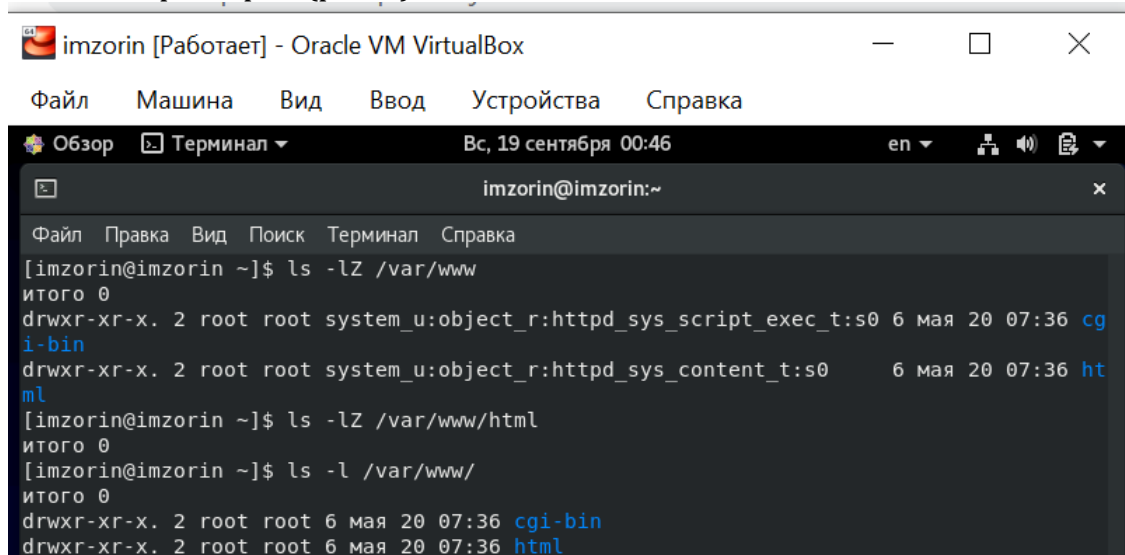
4. Посмотрел статистику по политике с помощью команды `seinfo`, также определил множество пользователей, ролей, типов (рис. 4).



```
imzorin [Работает] - Oracle VM VirtualBox
Файл  Машина  Вид  Ввод  Устройства  Справка
Обзор  Терминал  Вс, 19 сентября 00:42  en
imzorin@imzorin:~
Файл  Правка  Вид  Поиск  Терминал  Справка
[imzorin@imzorin ~]$ seinfo
Statistics for policy file: /sys/fs/selinux/policy
Policy Version:          31 (MLS enabled)
Target Policy:           selinux
Handle unknown classes:  allow
Classes:                  132      Permissions:             463
Sensitivities:            1      Categories:             1024
Types:                    4959    Attributes:             255
Users:                    8       Roles:                  14
Booleans:                 340     Cond. Expr.:            389
Allow:                    112885  Neverallow:              0
Auditallow:               166     Dontaudit:              10362
Type_trans:               253398  Type_change:             87
Type_member:              35      Range_trans:            6015
Role_allow:               38      Role_trans:             423
Constraints:              72      Validatetrans:           0
MLS Constrain:            72      MLS Val. Tran:           0
Permissives:              0       Polcap:                  5
Defaults:                 7       Typebounds:              0
Allowxperm:               0       Neverallowxperm:         0
Auditallowxperm:          0       Dontauditxperm:          0
Ibendportcon:             0       Ibpkeycon:               0
Initial SIDs:             27      Fs_use:                  33
Genfscon:                 106     Portcon:                 640
Netifcon:                 0       Nodecon:                 0
[imzorin@imzorin ~]$
```

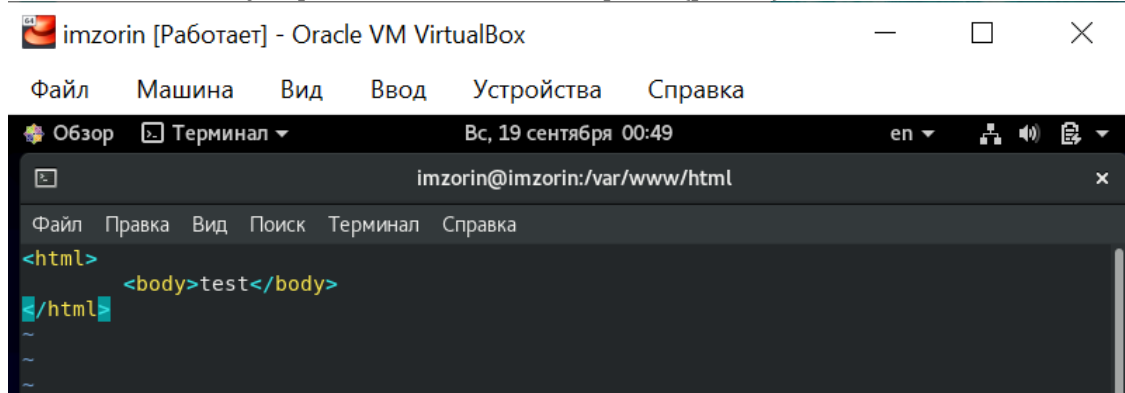
5. Определил тип файлов и поддиректорий, находящихся в директории `/var/www`. Определил тип файлов, находящихся в директории `/var/www/html`. Определил круг пользователей, которым разрешено создание

файлов в директории (рис. 5).



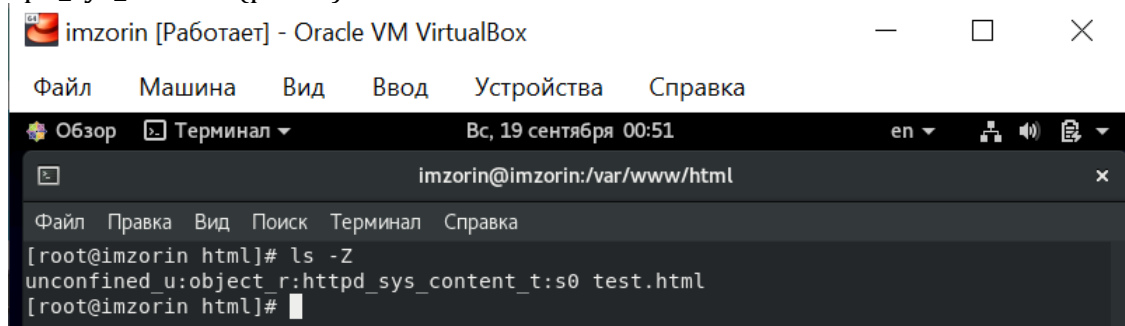
```
imzoring [Работает] - Oracle VM VirtualBox
Файл  Машина  Вид  Ввод  Устройства  Справка
Обзор  Терминал  Вс, 19 сентября 00:46  en  [иконки]
imzoring@imzoring:~
Файл  Правка  Вид  Поиск  Терминал  Справка
[imzoring@imzoring ~]$ ls -lZ /var/www
итого 0
drwxr-xr-x. 2 root root system_u:object_r:httpd_sys_script_exec_t:s0 6 мая 20 07:36 cgi-
bin
drwxr-xr-x. 2 root root system_u:object_r:httpd_sys_content_t:s0 6 мая 20 07:36 ht
ml
[imzoring@imzoring ~]$ ls -lZ /var/www/html
итого 0
[imzoring@imzoring ~]$ ls -l /var/www/
итого 0
drwxr-xr-x. 2 root root 6 мая 20 07:36 cgi-bin
drwxr-xr-x. 2 root root 6 мая 20 07:36 html
```

6. Создал от имени суперпользователя html-файл (рис. 6).



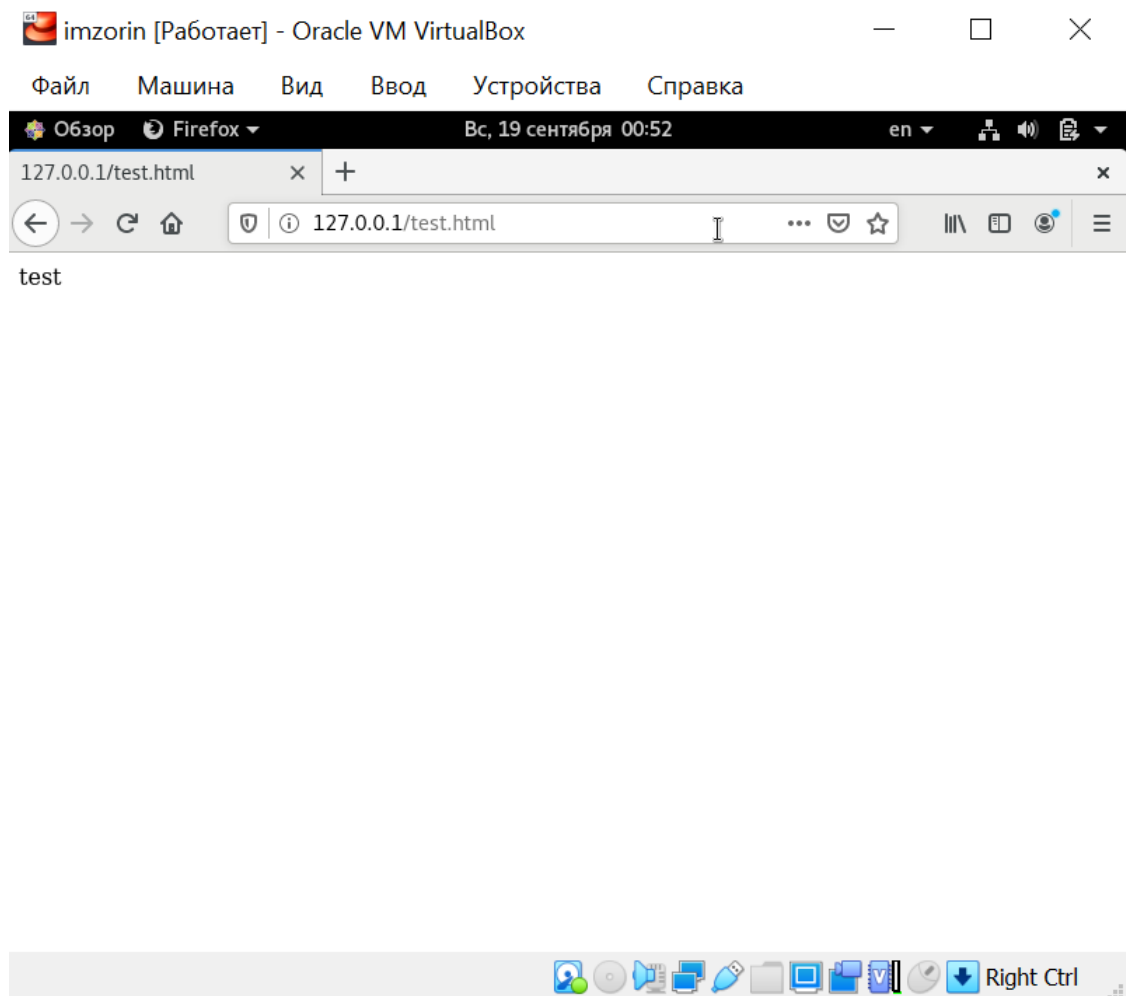
```
imzoring [Работает] - Oracle VM VirtualBox
Файл  Машина  Вид  Ввод  Устройства  Справка
Обзор  Терминал  Вс, 19 сентября 00:49  en  [иконки]
imzoring@imzoring:/var/www/html
Файл  Правка  Вид  Поиск  Терминал  Справка
<html>
  <body>test</body>
</html>
~
~
```

7. Проверил контекст созданного файла. Контекст, присваиваемый по умолчанию вновь созданным файлам в директории /var/www/html: httpd\_sys\_content (рис. 7).

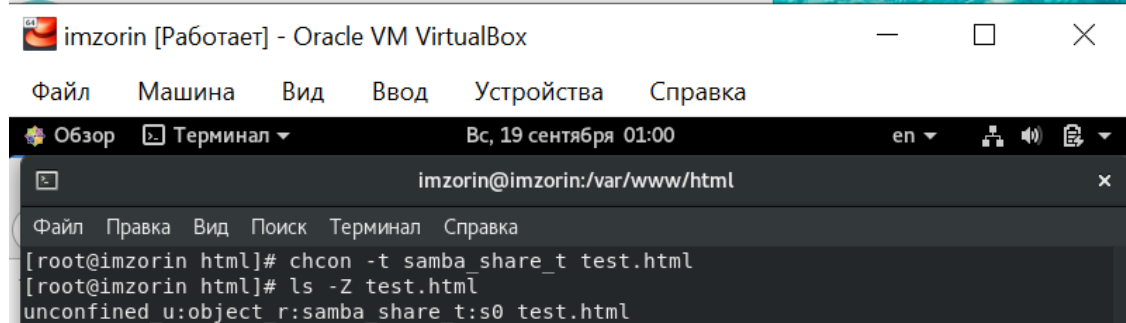


```
imzoring [Работает] - Oracle VM VirtualBox
Файл  Машина  Вид  Ввод  Устройства  Справка
Обзор  Терминал  Вс, 19 сентября 00:51  en  [иконки]
imzoring@imzoring:/var/www/html
Файл  Правка  Вид  Поиск  Терминал  Справка
[root@imzoring html]# ls -lZ
unconfined_u:object_r:httpd_sys_content_t:s0 test.html
[root@imzoring html]#
```

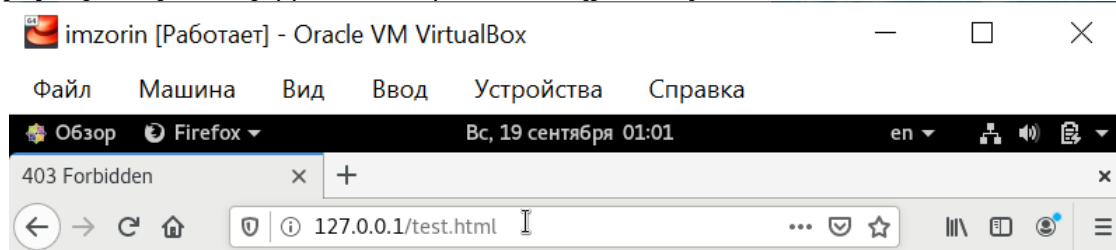
8. Обратился к файлу через веб-сервер, введя в браузере адрес `http://127.0.0.1/test.html`. Убедился, что файл успешно отображён (рис. 8).



9. Изменил контекст файла `/var/www/html/test.html` с `httpd_sys_content_t` на `samba_share_t`. После этого проверил, что контекст поменялся (рис. 9).



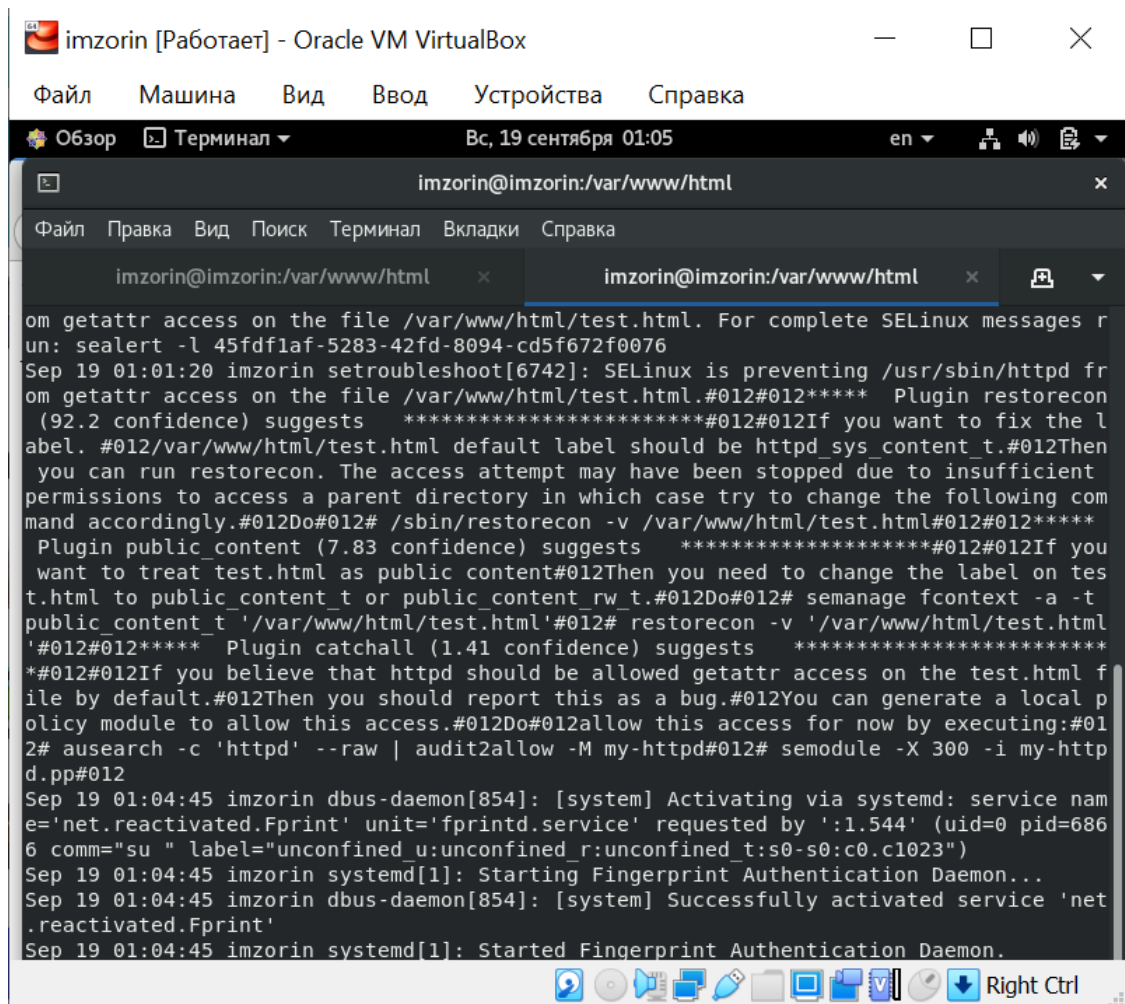
10. Попробовал ещё раз получить доступ к файлу через веб-сервер, введя в браузере адрес `http://127.0.0.1/test.html` (рис. 10).



## Forbidden

You don't have permission to access this resource.

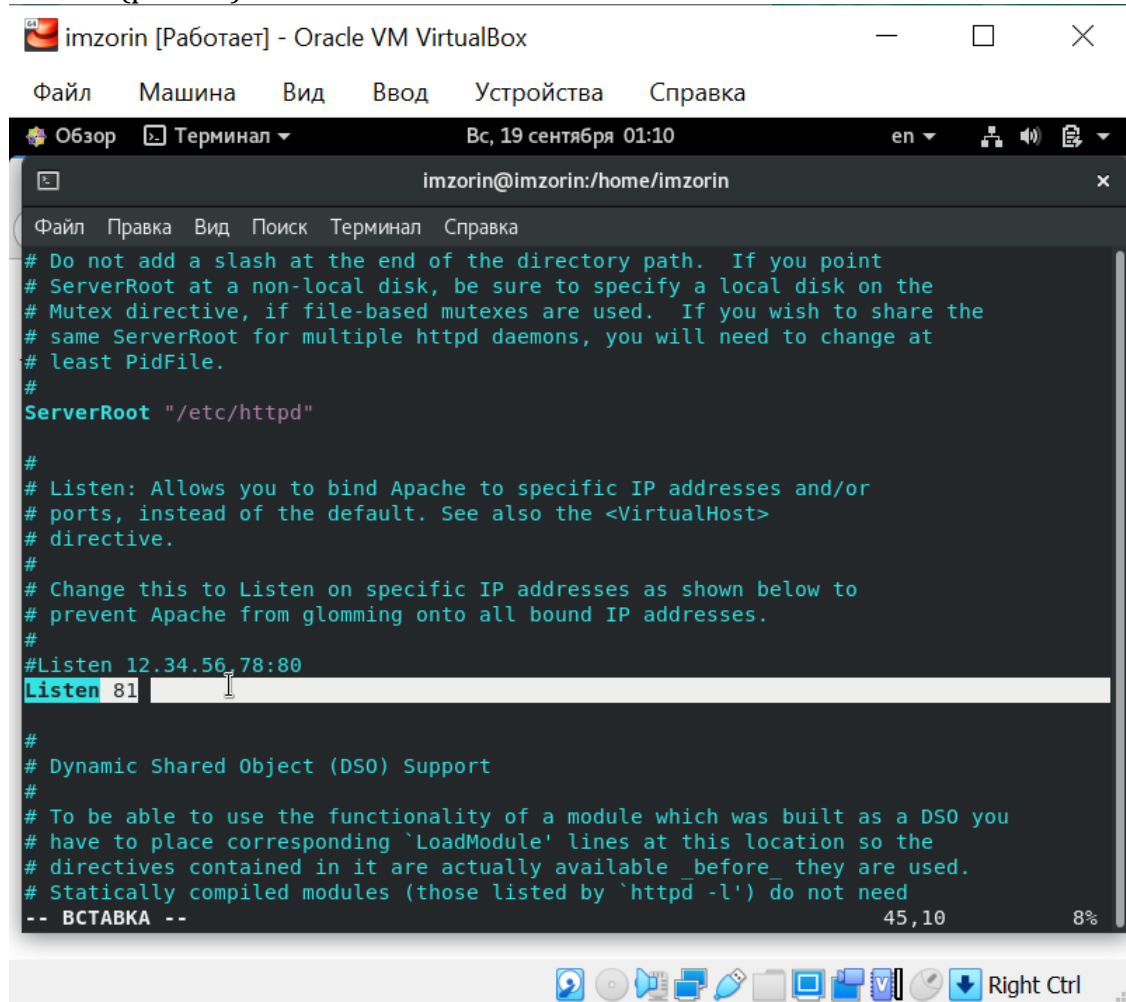
11. Проанализировал ситуацию. Почему файл не был отображён, если права доступа позволяют читать этот файл любому пользователю? Просмотрел log-файлы веб-сервера Apache. Также просмотрите системный лог-файл. Если в системе окажутся запущенными процессы `setroubleshootd` и `audtd`, то вы также сможете увидеть ошибки, аналогичные указанным выше, в файле `/var/log/audit/audit.log`. Проверьте это утверждение самостоятельно (рис. 11-12).





12. Попробовал запустить веб-сервер Apache на прослушивание TCP-порта 81. Для этого в файле /etc/httpd/httpd.conf нашёл строчку Listen 80 и заменил её на

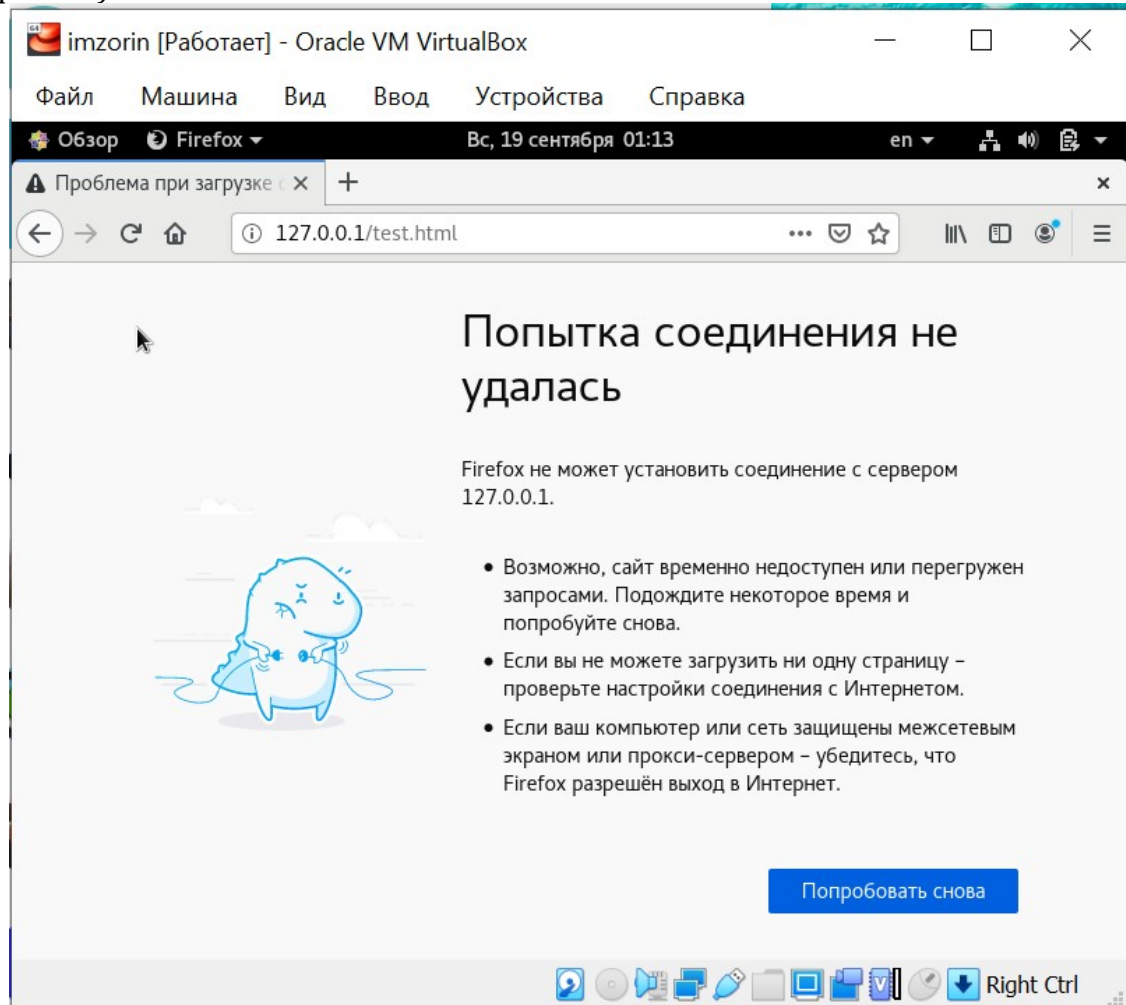
Listen 81 (рис. 13).



The screenshot shows a terminal window titled "imzorin [Работает] - Oracle VM VirtualBox". The terminal is running a shell with the prompt "imzorin@imzorin:/home/imzorin". The terminal displays the contents of the httpd.conf file, which includes comments about the Listen directive and the ServerRoot. The current line being edited is "Listen 81", where "Listen" is highlighted in blue and "81" is being typed. The terminal also shows the status bar at the bottom with "45,10" and "8%".

```
imzorin@imzorin:/home/imzorin
# Do not add a slash at the end of the directory path. If you point
# ServerRoot at a non-local disk, be sure to specify a local disk on the
# Mutex directive, if file-based mutexes are used. If you wish to share the
# same ServerRoot for multiple httpd daemons, you will need to change at
# least PidFile.
#
ServerRoot "/etc/httpd"
#
# Listen: Allows you to bind Apache to specific IP addresses and/or
# ports, instead of the default. See also the <VirtualHost>
# directive.
#
# Change this to Listen on specific IP addresses as shown below to
# prevent Apache from glomming onto all bound IP addresses.
#
#Listen 12.34.56.78:80
Listen 81
#
# Dynamic Shared Object (DSO) Support
#
# To be able to use the functionality of a module which was built as a DSO you
# have to place corresponding 'LoadModule' lines at this location so the
# directives contained in it are actually available _before_ they are used.
# Statically compiled modules (those listed by 'httpd -l') do not need
-- ВСТАВКА --
45,10 8%
```

13. Выполнил перезапуск веб-сервера Apache. Произошёл сбой. Поясните почему? (рис. 14).



14. Проанализировал лог-файлы. Просмотрел файлы `/var/log/http/error_log`, `/var/log/http/access_log` и `/var/log/audit/audit.log` и выясните, в каких файлах появились записи (рис. 15-18).

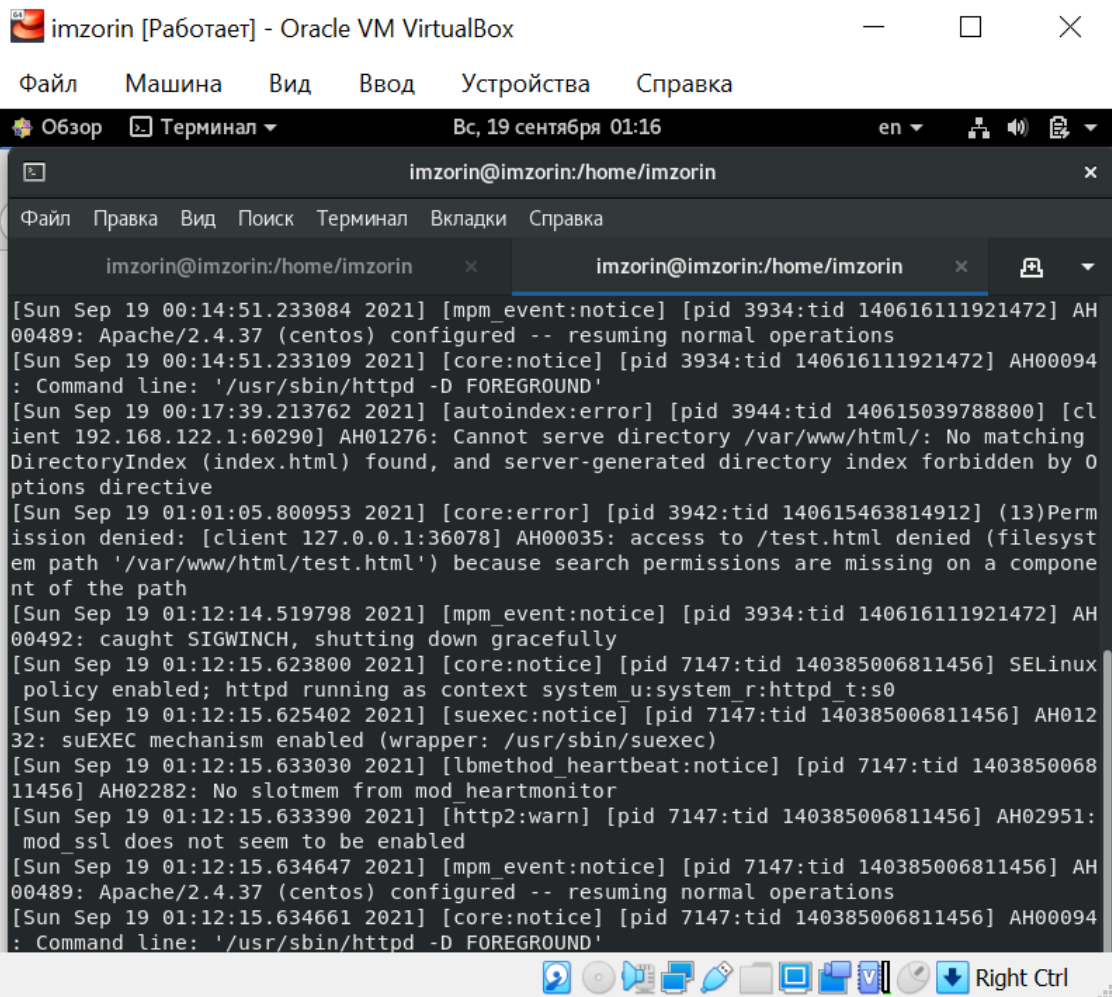
```
imzorin [Работает] - Oracle VM VirtualBox
Файл  Машина  Вид  Ввод  Устройства  Справка

Обзор  Терминал  Вс, 19 сентября 01:15  en  [иконки]

imzorin@imzorin:/home/imzorin
Файл  Правка  Вид  Поиск  Терминал  Вкладки  Справка

imzorin@imzorin:/home/imzorin  x  imzorin@imzorin:/home/imzorin  x  [иконки]

[imzorin@imzorin ~]$ su
Пароль:
[root@imzorin imzorin]# tail -nl /var/log/messages
tail: неверное число строк: «l»
[root@imzorin imzorin]# tail -l /var/log/messages
Sep 19 01:12:15 imzorin systemd[1]: Stopped The Apache HTTP Server.
Sep 19 01:12:15 imzorin systemd[1]: Starting The Apache HTTP Server...
Sep 19 01:12:15 imzorin httpd[7147]: Server configured, listening on: port 81
Sep 19 01:12:15 imzorin systemd[1]: Started The Apache HTTP Server.
Sep 19 01:14:27 imzorin dbus-daemon[854]: [system] Activating via systemd: service nam
e='net.reactivated.Fprint' unit='fprintd.service' requested by ':1.557' (uid=0 pid=743
9 comm="su " label="unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023")
Sep 19 01:14:27 imzorin systemd[1]: Starting Fingerprint Authentication Daemon...
Sep 19 01:14:27 imzorin dbus-daemon[854]: [system] Successfully activated service 'net
.reactivated.Fprint'
Sep 19 01:14:27 imzorin systemd[1]: Started Fingerprint Authentication Daemon.
Sep 19 01:14:29 imzorin su[7439]: (to root) imzorin on pts/1
Sep 19 01:14:58 imzorin systemd[1]: fprintd.service: Succeeded.
```



```
[root@imzorin log]# cat /var/log/httpd/access_log
192.168.122.1 - - [19/Sep/2021:00:17:39 +0300] "GET / HTTP/1.1" 403 199691 "-" "Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0"
192.168.122.1 - - [19/Sep/2021:00:17:39 +0300] "GET /poweredby.png HTTP/1.1" 200 10401 "http://192.168.122.1/" "Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0"
192.168.122.1 - - [19/Sep/2021:00:17:39 +0300] "GET /icons/poweredby.png HTTP/1.1" 200 643 "http://192.168.122.1/" "Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0"
127.0.0.1 - - [19/Sep/2021:00:52:22 +0300] "GET /test.html HTTP/1.1" 200 34 "-" "Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0"
127.0.0.1 - - [19/Sep/2021:00:52:22 +0300] "GET /favicon.ico HTTP/1.1" 404 196 "-" "Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0"
127.0.0.1 - - [19/Sep/2021:00:56:46 +0300] "GET /test.html HTTP/1.1" 200 34 "-" "Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0"
127.0.0.1 - - [19/Sep/2021:00:56:47 +0300] "GET /favicon.ico HTTP/1.1" 404 196 "-" "Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0"
127.0.0.1 - - [19/Sep/2021:01:01:05 +0300] "GET /test.html HTTP/1.1" 403 199 "-" "Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0"
[root@imzorin log]#
```



imzorin [Работает] - Oracle VM VirtualBox



Файл Машина Вид Ввод Устройства Справка

Файл Правка Вид Поиск Терминал Вкладки Справка

imzorin@imzorin:/home/imzorin

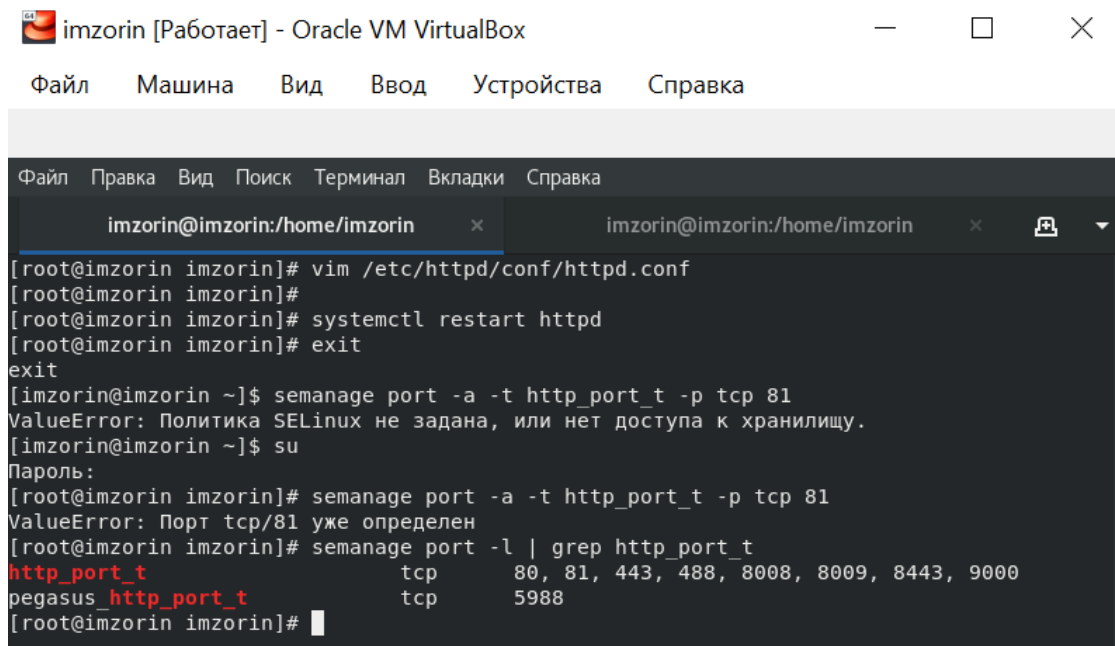
imzorin@imzorin:/home/imzorin

```
onfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023 msg='op=PAM:session_close grantors=pam_keyinit,pam_limits,pam_systemd,pam_unix,pam_umask acct="root" exe="/usr/bin/su" hostname=imzorin.localdomain addr=? terminal=pts/1 res=success' ID="imzorin" AUID="imzorin"
type=CRED_DISP msg=audit(1632003665.640:283): pid=7604 uid=1000 auid=1000 ses=3 subj=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023 msg='op=PAM:setcred grantors=pam_unix acct="root" exe="/usr/bin/su" hostname=imzorin.localdomain addr=? terminal=pts/1 res=success' ID="imzorin" AUID="imzorin"
type=SERVICE_START msg=audit(1632003690.167:284): pid=1 uid=0 auid=4294967295 ses=4294967295 subj=system_u:system_r:init t:s0 msg='unit=fprintd comm="systemd" exe="/usr/lib/systemd/systemd" hostname=? addr=? terminal=? res=success' ID="root" AUID="unset"
type=USER_AUTH msg=audit(1632003692.474:285): pid=7749 uid=1000 auid=1000 ses=3 subj=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023 msg='op=PAM:authentication grantors=pam_unix acct="root" exe="/usr/bin/su" hostname=imzorin.localdomain addr=? terminal=pts/1 res=success' ID="imzorin" AUID="imzorin"
type=USER_ACCT msg=audit(1632003692.475:286): pid=7749 uid=1000 auid=1000 ses=3 subj=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023 msg='op=PAM:accounting grantors=pam_unix,pam_localuser acct="root" exe="/usr/bin/su" hostname=imzorin.localdomain addr=? terminal=pts/1 res=success' ID="imzorin" AUID="imzorin"
type=CRED_ACQ msg=audit(1632003692.479:287): pid=7749 uid=1000 auid=1000 ses=3 subj=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023 msg='op=PAM:setcred grantors=pam_unix acct="root" exe="/usr/bin/su" hostname=imzorin.localdomain addr=? terminal=pts/1 res=success' ID="imzorin" AUID="imzorin"
type=USER_START msg=audit(1632003692.487:288): pid=7749 uid=1000 auid=1000 ses=3 subj=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023 msg='op=PAM:session_open grantors=pam_keyinit,pam_limits,pam_systemd,pam_unix,pam_umask acct="root" exe="/usr/bin/su" hostname=imzorin.localdomain addr=? terminal=pts/1 res=success' ID="imzorin" AUID="imzorin"
[root@imzorin imzorin]#
```



Right Ctrl

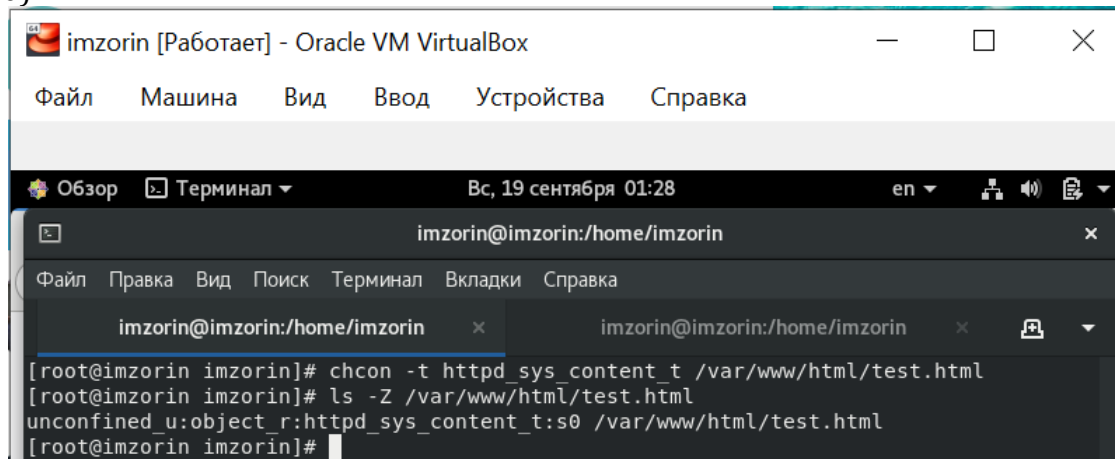
15. Выполнил команду `semanage port -a -t http_port_t -p tcp 81`. После этого проверил список портов. Убедился, что порт 81 появился в списке (рис. 19).



The screenshot shows a terminal window titled "imzorin [Работает] - Oracle VM VirtualBox". The terminal output is as follows:

```
imzorin@imzorin:/home/imzorin
[root@imzorin imzorin]# vim /etc/httpd/conf/httpd.conf
[root@imzorin imzorin]# systemctl restart httpd
[root@imzorin imzorin]# exit
exit
[imzorin@imzorin ~]$ semanage port -a -t http_port_t -p tcp 81
ValueError: Политика SELinux не задана, или нет доступа к хранилищу.
[imzorin@imzorin ~]$ su
Пароль:
[root@imzorin imzorin]# semanage port -a -t http_port_t -p tcp 81
ValueError: Порт tcp/81 уже определен
[root@imzorin imzorin]# semanage port -l | grep http_port_t
http_port_t          tcp      80, 81, 443, 488, 8008, 8009, 8443, 9000
pegasus_http_port_t  tcp      5988
[root@imzorin imzorin]#
```

16. Вернул контекст `httpd_sys_content_t` к файлу `/var/www/html/test.html` (рис. 20).

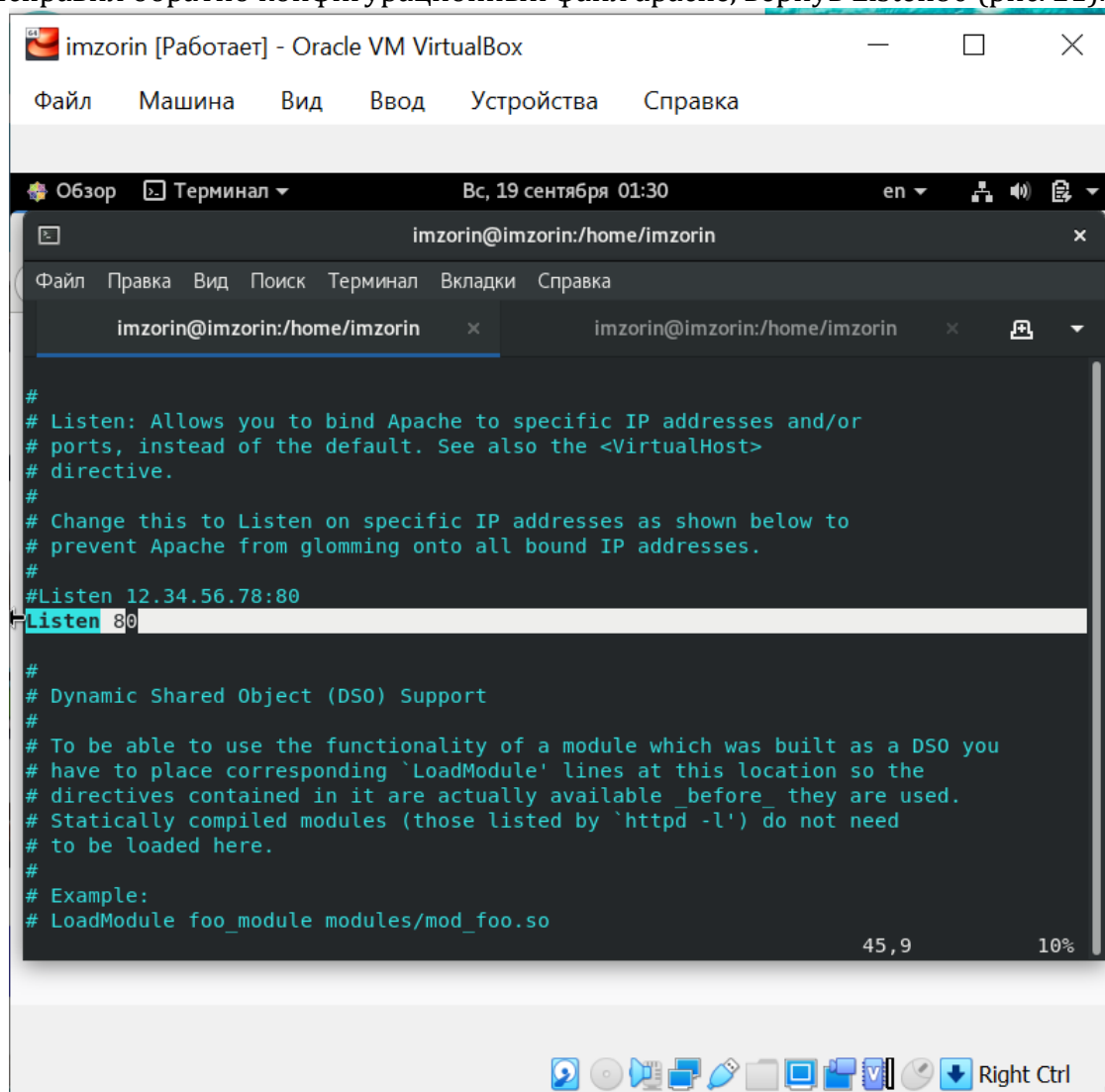


The screenshot shows a terminal window titled "imzorin [Работает] - Oracle VM VirtualBox". The terminal output is as follows:

```
imzorin@imzorin:/home/imzorin
[root@imzorin imzorin]# chcon -t httpd_sys_content_t /var/www/html/test.html
[root@imzorin imzorin]# ls -Z /var/www/html/test.html
unconfined_u:object_r:httpd_sys_content_t:s0 /var/www/html/test.html
[root@imzorin imzorin]#
```



17. Исправил обратно конфигурационный файл apache, вернув Listen80 (рис. 21).

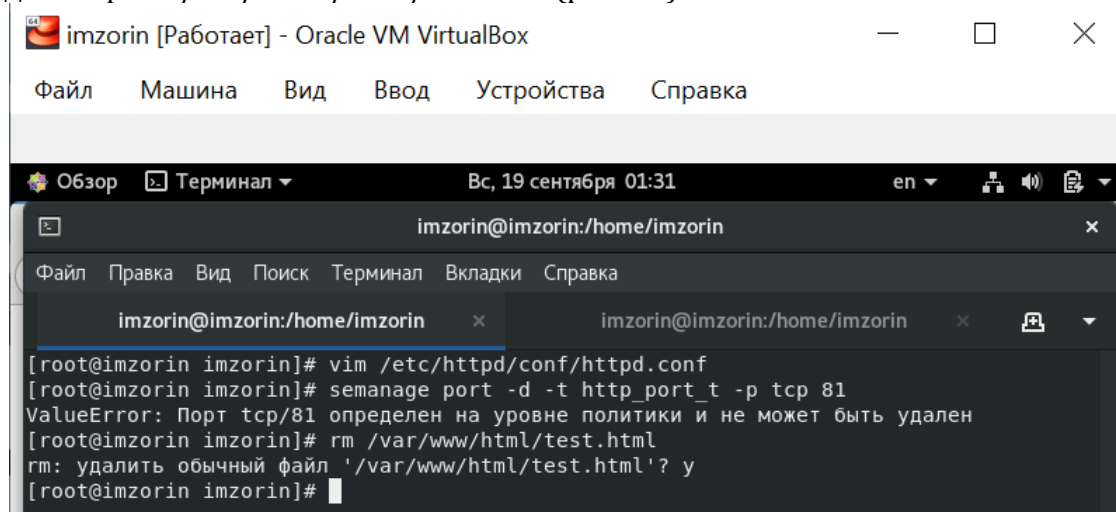


```
#
# Listen: Allows you to bind Apache to specific IP addresses and/or
# ports, instead of the default. See also the <VirtualHost>
# directive.
#
# Change this to Listen on specific IP addresses as shown below to
# prevent Apache from glomming onto all bound IP addresses.
#Listen 12.34.56.78:80
Listen 80

#
# Dynamic Shared Object (DSO) Support
#
# To be able to use the functionality of a module which was built as a DSO you
# have to place corresponding 'LoadModule' lines at this location so the
# directives contained in it are actually available _before_ they are used.
# Statically compiled modules (those listed by 'httpd -l') do not need
# to be loaded here.
#
# Example:
# LoadModule foo_module modules/mod_foo.so
```



18. Удалил привязку http\_port\_t к 81 порту и проверил, что порт 81 удалён. Удалил файл /var/www/html/test.html (рис. 22).



The screenshot shows a terminal window titled "imzorin [Работает] - Oracle VM VirtualBox". The terminal output is as follows:

```
imzorin@imzorin:/home/imzorin
[root@imzorin imzorin]# vim /etc/httpd/conf/httpd.conf
[root@imzorin imzorin]# semanage port -d -t http_port_t -p tcp 81
ValueError: Порт tcp/81 определен на уровне политики и не может быть удален
[root@imzorin imzorin]# rm /var/www/html/test.html
rm: удалить обычный файл '/var/www/html/test.html'? y
[root@imzorin imzorin]#
```

## Выводы

Развил навыки администрирования ОС Linux. Получил первое практическое знакомство с технологией SELinux. Проверил работу SELinux на практике совместно с веб-сервером Apache.